Outline

Quantum circuits

Clifford+T and universal gate sets

CNOT-dihedral gates

Rules for CNOT-dihedral gates

Normal forms

Phase polynomials and uniqueness

Phase polynomials

Action of a diagonal gate:

$$D\left|x\right\rangle = \omega^{p_D(x)}\left|x\right\rangle, \quad p_D : \mathbb{Z}_2^n \to \mathbb{Z}_8,$$

$$p_D(x) = \sum_{i=1}^{k} a_i g_i(x).$$

where $a_i \in \mathbb{Z}_8$ and $g_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$ are terms on at most n variables.

$$\omega^k\left|x\right\rangle = \omega^k\left|x\right\rangle$$

$$T^k\left|x_1\right\rangle = \omega^{kx_1}\left|x_1\right\rangle$$

$$U^k\left|x_1x_2\right\rangle = \omega^{k(x_1\oplus x_2)}\left|x_1x_2\right\rangle$$

$$V^k\left|x_1x_2x_3\right\rangle = \omega^{k(x_1\oplus x_2\oplus x_3)}\left|x_1x_2x_3\right\rangle$$

Therefore for D in normal form we have

$$p_D(x) = a_0 + \sum_i a_i x_i + \sum_{i<j} b_{ij}(x_i \oplus x_j) + \sum_{i<j<k} c_{ijk}(x_i \oplus x_j \oplus x_k)$$

Uniqueness

Suppose D and D' are distinct diagonal normal forms, then by construction $p_D(x) \neq p_{D'}(x)$ as polynomials. However this does not mean that $\exists y \in \mathbb{Z}_2^n$ s.t. $p_D(y) \neq p_{D'}(y)$.
Counterexample: $4x_1 + 4x_2 + 4(x_1 \oplus x_2) = 0 \bmod 8$ for any $x_1, x_2 \in \mathbb{Z}_2$
To show there exists such a y need a technical lemma: construct a multilinear polynomial $q : \mathbb{Z}_8^n \to \mathbb{Z}_8$ such that $p_D(y) - p_{D'}(y) = q(y)\ \forall y \in \mathbb{Z}_2^n$.
Do this by translating from mod 2 to mod 8:

$$x_i \oplus x_j = x_i + x_j - 2x_i x_j$$

$$x_i \oplus x_j \oplus x_k = x_i + x_j + x_k - 2x_i x_j \ldots$$

Then $p_D(x) - p_{D'}(x) \neq 0 \implies q(x) \neq 0$, we pick a non-zero term $dx_{i_1} \ldots x_{i_k}$ in $q(x)$ then letting y be the vector with 1's in i_jth positions and zero everywhere else we obtain $q(y) = d \neq 0$ and so $D\,|y\rangle \neq D'\,|y\rangle$.